MBONED Working Group
Internet-Draft
Intended status: Informational
Expires: September 7, 2011

H. Asaeda
Keio University
V. Roca
INRIA

March 6, 2011

Limitations of Session Announcement Protocol (SAP) draft-asaeda-mboned-sap-limitation-00

Abstract

The Session Announcement Protocol (SAP) [2] has historically been used to announce information for all available IP multicast sessions to the prospective receivers in the experimental MBone. Each receiver can then discover which sessions are available and which ones he may want to join. Although SAP is easy to use, SAP is not scalable and controlling the SAP message transmission in a wide area network is not easy. Therefore this document describes the limitations of SAP when used in the global Internet. Furthermore, SAP has recently been used as a convenient method for conveying configuration information to a set of receivers that are already interested by a multicast session (e.g., to carry FEC Framework Configuration Information [7]). This documents describes the limitations of SAP for this type of usage, since this latter is rather different from its original goals.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 7, 2011.

Copyright Notice

Table of Contents

1. Introduction

1.1. SAP as a Component of a Session Discovery Mechanism

Session configuration information (e.g., IP multicast session or channel information) can be described with the Session Description Protocol (SDP) [3] syntax, or written in a metafile whose format has been defined elsewhere. The Session Announcement Protocol (SAP) [2] has been used to announce information for all available multicast sessions to the prospective receivers in the experimental MBone. In a SAP announcement procedure, the entire session information must be periodically transmitted and all active session descriptions must be continuously refreshed. If ever a session is no longer announced, its description eventually times out and is deleted from the available session list (this is a "soft-state" protocol).

SAP enables to keep the session information active by periodically refreshing it, and it provides a robust and fault-tolerant system. However, it requires the periodic message transmission (i.e., message flooding) that may cause major overheads or overloads. Although this strategy keeps the implementation simple, it rises significant overheads which further reduces its scalability.

Another issue is closely related to a security or policy management. Indeed, using SAP and existing scoping techniques make it difficult to control precisely the amount of traffic distributed as well as the distribution area itself.

This document describes the limitations of SAP when used in the global Internet, inspired by the work originally published by the authors in [6].

1.2. SAP as a Component of a Configuration Information Transport Mechanism

More recently SAP has been used as a convenient method for conveying configuration information to a set of receivers that are already interested in a multicast session (e.g., these receivers have obtained the content description through another mechanism and have decided to join the session). For instance SAP can be used to convey the FEC Framework Configuration Information (FFCI) of a given FECFRAME Instance [7]. The FFCI is the information that the FEC Framework needs in order to apply FEC protection to the upper application flows [8]. Said differently, this FFCI defines the way the packets containing encoding symbols (e.g., result of a Reed-Solomon encoding) are generated from one or several upper application flows (e.g., an RTP stream containing video). This use-case is significantly different from the traditional one since the receivers

have already expressed their interest in joining the FECFRAME Instance session and now need to collect additional information on how to exploit the associated flow(s).

This document describes the limitations of SAP for this type of usage that is rather different from the original goals of SAP.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED","MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3. Potential Limitations with SAP

3.1. Announcement Interval vs. Latency (SAP as a Session Discovery Mechanism)

SAP improves the robustness and data consistency in front of packet losses by periodically transmitting SAP messages. However, transmitting a large number of SAP messages with active multicast session information in a flooding manner may cause major overheads. The solution defined in [2] is the time period between repetitions of an announcement. This period is chosen such that the total bandwidth used by all announcements on a single SAP group remains below a preconfigured limit, and the bandwidth limit should be assumed to be 4000 bits per second, if not specified.

However, this solution largely increases the latency experienced by end users especially when the number of sessions increases. In its definition, since the minimum interval of SAP message transmission is 200 seconds, end users experience a minimum waiting time of 200 seconds to obtain the entire session list, irrespective of the number of observed multicast sessions, message size of multicast session information, and bandwidth SAP uses. Let us assume the average message size of a single multicast session information is about 300 bytes. When there are more than 500 active multicast sessions, an interval time of each session announcement becomes greater than 200 seconds and the average announcement interval increases accordingly. For instance, if 2000 multicast sessions are active in the Internet, each session announcement interval is between 800 seconds and 1600 seconds. In this case, if some SAP message is lost, users may need to wait 1600 seconds for the next announcement as maximum.

Obviously, it is possible to make the announcement interval shorter by changing the SAP configuration on a sender side and provide

shorter latency for the sender-receiver communication. However, it makes the total amount of SAP messages transmitted larger and may increase the probability of creating congestions.

3.2. Announcement Interval vs. Latency (SAP as a Configuration Information Transport Mechanism)

Using SAP as a configuration information transport mechanism raises the problem of choosing an appropriate announcement interval. The goal of the algorithm introduced in [2] is to control SAP transmission overhead, in particular when the number of active sessions is high and generates a large number of announcements. When SAP is used as a configuration information transport mechanism, the problem is totally different, since SAP is used within a given session and the goal is to ensure that all receivers, including late-comers, retrieve the configuration information (e.g., the FEC Framework Configuration Information) in a timely manner. To achieve this goal it is desired to set up periodic transmissions. For instance, [7] suggests a time interval in the range of 1 - 200 seconds that defaults to 60 seconds (to be compared to the one hour minimum implicit timeout duration of SAP). SAP SHOULD enable such a flexibility when defining the announcement interval strategy.

A receiver SHOULD be able to determine the validity period of each SAP announcement, since SAP entries are cached by the reaceiver and are automatically discarded at timeout. SAP specifies that the announcement interval can be predicted by the receiver and defines a minimum of one hour for an implicit timeout of the entries, with the goal to allow for transient network partitionings (as described in section 4 of [2]). This approach contradicts the goal of precisely controlling the announcement interval strategy with a possibility to use intervals in the range of a few seconds. Therefore, a solution could be for the SAP sender to communicate the announcement interval being used to the receivers. The current SAP specification does not allow the time-interval to be signaled in the SAP header which requires to include this information within the payload itself (given in [7]), making the technique dependant on the configuration information being transported which is not a desired property.

3.3. Difficulties in Scope Definition (both SAP Uses)

Multicast data senders or network administrators may want to define an area where data packets sent within a session will be confined. This area is called "scope area" and the end users who belong to this scope area are the only ones who can receive the session data.

When IP multicast was initially deployed in the MBone, the Time-To-Live (TTL) field of the IP header was used to control the

distribution of multicast traffic. A multicast router configured with a TTL threshold drops any multicast packet in which the TTL falls below the threshold. For instance, a router at the boundary of an organization configures the threshold to 32, which denotes an "organization" scope boundary.

The drawbacks of this "TTL scoping" are: 1) the senders must be sufficiently aware of the network topology to determine the TTL value to use, and 2) complex scope areas cannot be defined (e.g., between overlapped areas). Especially the first point becomes big obstacles for general end users to precisely set up the data distribution area. TTL scoping, which only defines a rough granularity, does not provide a complete solution.

The "administratively scoped IP multicast" approach [4] provides clear and simple semantics and scope boundaries are associated to multicast addresses. With IPv4, packets addressed to the administratively scoped multicast address range 239/8 (i.e., from 239.0.0.0 to 239.255.255.255) cannot cross the configured administrative boundaries. Since scoped addresses are defined locally, the same multicast address can be used in different non-overlapping areas. Oppositely, an administrator can define multiple areas that overlap by dividing the administratively scoped address range, which is not possible with TTL scoping.

However, administrative scoping has several major limitations. An administrator may want to partition the scope area to disjoint areas on a per receiver basis, or he may want to limit data distribution according to the transmission rate or the content category of each session, or he may want to use the data sender's address as a keyword to set up the scope. Note that the latter aspect is nowadays feasible since Source-Specific Multicast (SSM) [5] requires that a join request specifies both the multicast and source addresses.

SSM highlights another contradiction in the administrative scoping approach: the address range dedicated to SSM, 232/8 with IPv4, cannot cover the address range dedicated to administrative scoping, 239/8. Although the problem can be solved by defining yet another SSM specific administrative scoping address range, defining a new addressing architecture requires modifying application, end host, and router implementations or configurations. Hence, using multicast addresses to define a scope is not a complete solution either.

3.4. ASM Dependency (both SAP Uses)

SAP relies on the ASM model, since every SAP instance can send announcements in the SAP announcement group. For instance, to receive SAP announcement messages for the global scope IPv4 multicast

sessions, all prospective receivers must join session 224.2.127.254 (without specifying any source address). This is another major limitation of SAP since some Internet Service Providers (ISPs) may want to provide only SSM multicast routing. It is known that a versatile announcement protocol should not rely on any specific routing architecture.

Moreover, this communication model is subject to a Denial-of-Service attack. If malicious hosts flood high bandwidth stream to this global announcement address, 224.2.127.254, then all prospective receivers and multicast routers that listen to SAP messages will receive this high bandwidth flow which will impact their own performance and that of their network.

3.5. Lack of Sender and Receiver Control during Announcements (both SAP Uses)

Network administrators or service providers may want to define approved senders and restrict multicast data transmissions or announcement only from them. However, in a spontaneous announcement protocol, it is impossible to allow to send announcement messages only from approved senders or make non-approved senders stop sending announcement messages.

In addition, it is difficult to hide multicast session information announced by an announcement protocol from non-approved receivers if they are inside the scoped network. For instance, SAP messages might be encrypted to prevent non-authorized client from reading them. However, it adds more complexity to SAP by combining with additional key sharing mechanism.

Conceptually, it is difficult to disallow non-approved data receivers to receive session information announced by an announcement protocol, if the announcement data is flooded to their network. It is the basic concept that IP multicast requires scoping configuration to address this issue. However, defining a fine-grained scope areas with using TTL or a multicast address range is a big challenge as described in Section 3.3.

4. Security Considerations

TBD

5. IANA Considerations

This document does not require any action from IANA.

6. Acknowledgments

TBD

7. References

7.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[2] Handley, M., Perkins, C., and E. Whelan, "Session Announcement Protocol", RFC 2974, October 2000.

[3] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[4] Mayer, D., "Administratively scoped IP multicast", RFC 2365, July 1998.

[5] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

7.2. Informative References

[6] Asaeda, H. and V. Roca, "Policy and Scope Management for Multicast Channel Announcement", IEICE Trans. on Information and Systems, Vol.E88-D, No.7, pp.1638-1645, July 2005.

[7] Asati, R., "Methods to convey FEC Framework Configuration Information", draft-ietf-fecframe-config-signaling-04 (Work in Progress), January 2011.

[8] Watson, M., Begen, A., and V. Roca, "Forward Error Correction (FEC) Framework", draft-ietf-fecframe-framework-13 (Work in Progress), February 2011.

Authors' Addresses

Hitoshi Asaeda
Keio University
Graduate School of Media and Governance
5322 Endo
Fujisawa, Kanagawa 252-0882
Japan

Email: asaeda@wide.ad.jp
URI: http://www.sfc.wide.ad.jp/~asaeda/

Vincent Roca
INRIA
655, av. de l'Europe
Inovalle; Montbonnot
ST ISMIER cedex 38334
France

Email: vincent.roca@inria.fr
URI: http://planete.inrialpes.fr/people/roca/